VERSION OF AMENDED CLAIMS
WITH MARKINGS TO SHOW CHANGES MADE[1]

1. (Once Amended) A method for authenticating an electronic payment comprising:

receiving from a seller an electronic sales draft including an electronic signature;

receiving from said seller a digital certificate associated with a buyer, said digital certificate including a verification key and an encrypted version of a personal identification number (PIN);

using said verification key to verify that said electronic signature was authorized by said buyer;

extracting said encrypted version of said PIN from said digital certificate;

decrypting said encrypted version of said PIN;

generating, using said PIN, an authorization request;

sending said authorization request [for a PIN] to a financial institution;

receiving an approval of said authorization request from said financial institution; and

sending said approval to said seller.

2. (Once Amended) A method for authorizing an electronic purchase in a networked computer environment, comprising the steps of:

(a) receiving, from a merchant, a transaction authorization request including a digital certificate passed through said merchant from a user involved in said transaction,

[1] Applicant notes for the record that the foregoing amendments have the effect of broadening every claim – because originally recited language was deleted from every independent claim – so that the doctrine of prosecution history estoppel should be inapplicable.

(i) said digital certificate including a financial account datum associated with said user[, at least a portion of which is confidential from said merchant],

(ii) said digital certificate conveying a binding between at least a portion of said financial account datum and a public key of said user;

(b) verifying said binding using a cryptographic verification key associated with a trusted party performing said binding; and

(c) using said financial account datum to authorize a transaction order digitally signed by said user with a private key corresponding to said public key.

15. (Once Amended) A method for providing electronic payment capabilities to a user in a networked computer environment, comprising the steps of:

(a) obtaining a financial account datum associated with said user;

(b) obtaining a public key associated with said user;

(c) obtaining a cryptographically assured binding of said public key to at least a portion of said financial account datum,

(i) said binding being conveyed in a digital certificate for said user,

(ii) said digital certificate being usable by said user to conduct an electronic transaction involving said financial account datum; and

(d) transmitting said digital certificate to said user, enabling said user to conduct said electronic transaction involving (i) a merchant [from whom at least a portion of said financial account datum is kept confidential], and (ii) a transaction processor capable of verifying said binding using a cryptographic verification key associated with a trusted party performing said binding.

30. (Once Amended) An apparatus for authorizing an electronic purchase in a networked computer environment, comprising:

(a) a computer processor;

(b) a memory connected to said processor storing a program to control the operation of said processor;

(c) the processor operable with said program in said memory to:

(i) receive, from a merchant, a transaction authorization request, said request including a digital certificate passed through said merchant from a user involved in said transaction,

(1) said digital certificate including financial account datum associated with said user[, at least a portion of which datum is confidential from said merchant],

(2) said digital certificate conveying a binding between at least a portion of said financial account datum and a public key of said user;

(ii) verify said binding using a cryptographic verification key associated with a trusted party performing said binding; and

(iii) use said financial account datum to authorize a transaction order digitally signed by said user with a private key corresponding to said public key.

34. (Once Amended) An apparatus for providing electronic payment capabilities to a user in a networked computer environment, comprising:

(a) a processor;

(b) a memory connected to said processor storing a program to control the operation of said processor;

(c) the processor operable with said program in said memory to:

(i) obtain a financial account datum regarding said user,

(ii) obtain a public key associated with said user,

(iii) obtain a cryptographically assured binding of said public key to at least a portion of said financial account datum,

(1) said binding being conveyed in a digital certificate for said user,

(2) said digital certificate being usable by said user to conduct an electronic transaction involving said financial account datum, and

(iv) transmit said digital certificate to said user, enabling said user to conduct said electronic transaction involving (1) a merchant [from whom at least a portion of said financial account datum is kept confidential], and (2) a transaction processor capable of verifying said binding using a cryptographic verification key associated with a trusted party performing said binding.

38. (Once Amended) A computer-readable storage medium encoded with processing instructions for implementing a method for authorizing an electronic purchase in a networked computer environment, said processing instructions for directing a computer to perform the steps of:

(a) receiving, from a merchant, a transaction authorization request, said request including a digital certificate passed through said merchant from a user involved in said transaction,

(i) said digital certificate including a financial account datum associated with said user[, at least a portion of which datum is confidential from said merchant],

(ii) said digital certificate conveying a binding between at least a portion of said financial account datum and a public key of said user;

(b) verifying said binding using a cryptographic verification key associated with a trusted party performing said binding; and

(c) using said financial account datum to authorize a transaction order digitally signed by said user with a private key corresponding to said public key.

42. (Once Amended) A computer-readable storage medium encoded with processing instructions for implementing a method for providing electronic payment capabilities to a user in a networked computer environment, said processing instructions for directing a computer to perform the steps of:

(a) obtaining a financial account datum regarding said user;

(b) obtaining a public key associated with said user;

(c) obtaining a cryptographically assured binding of said public key to at least a portion of said financial account datum,

(i) said binding being conveyed in a digital certificate for said user,

(ii) said digital certificate being usable by said user to conduct an electronic transaction involving said financial account datum; and

(d) transmitting said digital certificate to said user, enabling said user to conduct said electronic transaction involving (i) a merchant [from whom at least a portion of said financial account datum is kept confidential], and (ii) a transaction processor capable of verifying said binding using a cryptographic verification key associated with a trusted party performing the said binding.

46. (Once Amended) A digital certificate for use in an electronic payment transaction in a networked computer environment, comprising:

(a) a financial account datum associated with a user[, at least a portion of which datum is confidential from a merchant involved in said payment transaction];

(b) a cryptographically assured binding of a public key associated with said user to at least a portion of said financial account datum, said binding having been generated with a cryptographic verification key associated with a trusted party performing said binding;

(c) said digital certificate configured for use by a transaction processor to:

(i) verify said binding using a cryptographic verification key associated with said trusted party, and

(ii) access said financial account datum to authorize a transaction order digitally signed with said user's private key corresponding to said public key.

59. (New) The method of claim 2 where at least a portion of said financial account datum is kept confidential from said merchant.

60. (New) The method of claim 15 where at least a portion of said financial account datum is kept confidential from said merchant.

61. (New) The method of claim 30 where at least a portion of said financial account datum is kept confidential from said merchant.

62. (New) The method of claim 34 where at least a portion of said financial account datum is kept confidential from said merchant.

63. (New) The method of claim 38 where at least a portion of said financial account datum is kept confidential from said merchant.

64. (New) The method of claim 42 where at least a portion of said financial account datum is kept confidential from said merchant.

65. (New) The method of claim 46 where at least a portion of said financial account datum is kept confidential from said merchant.

**** Remainder of Page is Blank****

REMARKS

A. No Narrowing Claim Amendments

Independent claims 1, 2, 15, 30, 34, 38, 42 & 46 have been amended. These amendments broaden the claims as originally presented by deleting certain language therefrom. New dependent claims 59-65 have been added via amendment. These claims merely restate what was previously presented in the underlying independent claims. Thus, none of the pending claims has been narrowed in any way, and Applicant wishes to state for the record that prosecution history estoppel should be inapplicable during any subsequent construction of any of the currently pending claims before a court or other body of competent jurisdiction.

B. Claim Rejections

The Examiner cited the abstract and col. 4, lines 32-65 of Slater as anticipating claims 1-58.

As to claim 1, no portions of Slater were specifically cited against the claim, leading the Applicant to believe that the rejection of claim 1 may have been inadvertent.

Applicant respectfully submits that the cited text does not teach multiple limitations of each of claims 2-58. In particular, the cited text does not disclose:

(1) a digital certificate of a user;

(2) the user's digital certificate being conveyable to a transaction processor via a merchant;

(3) the user's digital certificate conveying a binding between at least a portion of the user's financial account information and the user's public key; and

(4) enabling the transaction processor to verify the binding using a cryptographic verification key associated with a trusted party that performed the binding.

More specifically, the abstract of Slater was cited for limitation (1), but a word search of the abstract did not disclose the term "digital certificate." Further, the only mention of "digital certificate" in the cited text is a digital certificate of the merchant (col. 4, lines 60-61) – but not of the user.

The abstract was also cited for limitation (2), but the abstract does not disclose conveying a user's digital certificate to a transaction processor via a merchant. This follows from (1) above.

As to limitation (3), the cited text does not disclose cryptographically binding the user's public key to a portion of the user's account information, via the user's digital certificate. For example and without limitation, cryptographic binding would cover encrypting the two quantities under a domain key (or key pair) shared between the issuer proxy (independent claims 15, 34, 42) and the bridge computer (independent claims 2, 30, 38) into digital certificate for the user. Even if Slater disclosed a user's digital certificate, or assuming for the sake of argument that such a digital certificate were combinable with Slater from other background art, conventional digital certificates only encrypt the user's public key per se -- rather than binding that public key to the user's financial information.

As to limitation (4), since there is no disclosed binding, there can be no verification of the binding.

For these reasons, Applicant respectfully requests that the rejections be withdrawn and the claims passed to allowance.

If the Examiner believes that the prosecution of the application can be expedited through further discussions, the Examiner is invited to call the Applicant's attorney, Joe Yang, at (650) 470-4565.

Respectfully submitted,

Date: August 13, 2002

Joseph Yang
Reg. No. 41, 387

SKADDEN, ARPS, SLATE, MEAGHER & FLOM LLP
525 University Avenue
Palo Alto, California 94301